საქართველოს იუსტიციის სამინისტრო

კიბერ უსაფრთხოების საინფორმაციო ბიულეტინი: № 001
პოლიტიკა: ვებ საიტების იერარქიული აგებულება

IT ინფრასტრუქტურის დეპარტამენტი

სარჩევი:

შესავალი

საიტის იერარქიული სტრუქტურის არსებობა წამოადგენს მთავარ ასპექტს ვებ საიტების ჰოსტინგ ინფრასტრუქტურაში. ცუდად დაგეგმილმა იერარქიულმა პრინციპმა შეიძლება გამოიწვიოს მთელი რიგი პრობლემები ვებ საიტების მუშაობის დროს, რომლებიც ქვემოთ იქნება ჩამოთვლილი.
ყველა პირი ვინც მონაწილეობას ღებულობს ჰოსტინგ ინფრასტრუქტურაში არსებული საიტების შექმნაში, მოდიფიცირებაში, მხარდაჭერაში, ან ვებ სერვისების უზრუნველყოფაში, ვალდებულია დაიცვას ქვემოთ ჩამოთვლილი პირობები და პასუხისმგებელია მის მიერ შესრულებულ სამუშაოზე.

2. პოლიტიკის მიზნობრიობა

პოლიტიკის მიზანია დადგინდეს ვებ საიტის მკაცრად განსაზღვული იერარქიული პრინციპი, რომლის მიხედვითაც დამზადდება/ შეიმნება ახალი ვებ საიტი, ან მოდიფიცირდება არსებული. რადგანაც ერთიანი იერარქიული გეგმის არ არსებობის შემთხვევაში არსებობს შემდეგი პრობლემები:

- საიტის ტოტალური კონტროლოს მოპოვება შემტევის მიერ;
- Upload Code injection* შეტევა;
- ვებ ინფრასტრუქტურის მართვის გართულება;
- უსაფრთხოების საკითხების მოუგვარებლობა;
- მზარდი კიბერ საშიშროების რისკი (საიტების ზრდასთან ერთად);
- სისტემის მწყობრიდან გამოსვლის შემთხვევაში, მისი დროული აღდგენის შეუძლებლობა;
- მთლიანად, როგორც ვებ ინფრასტრუქტურის მოუქნელობა;
- მონიტორინგის და „ალერტინგის“ არ არსებობა.
- სერვერულ/ქსელური რესურსების არაეფექტური გამოყენება;

3 ვის ეხება აღნიშნული პოლიტიკა?

აღნიშნული საინფორმაციო ბიულეტინი ეხება ყველა იმ დეველოპერს, რომელიც მონაწილეობას ღებულობს საქართველოს იუსტიციის სამინისტროს მიერ დაკვეთილ ვებ საიტის/რესუსრის შექმნაში, ან არსებული საიტის მოდიფიკაციასა და პერიოდულ განახლებში, რომლებიც განთავსდება ამავე სამინისტროს დაცულ ვებ ჰოსტინგ ინფრსტრუქტურაში.

4. კონფიდენციალურობა და უსაფრთხოება

აღნიშნული პოლიტიკის მიხედვით დადგენილი პირობები აუდიტირდება პერიოდულად.

აღნიშნული პოლიტიკის დარღვევის და მისი უგულველყოფა-არშესრულების დროს საქართველოს იუსტიციის სამინისტროს შეუძლია მიმართოს შიდა განაწესით მიღებულ ზომებს.

5 . იერარქიული სტრუქტურა

ფაილების და დირექტორიების განლაგება უნდა შეესაბამებოდეს შემდეგ იერარქიულ პრინციპს:

საიტის მართვის პანელის დირექტორია: **/var/www/<site.ge>/manage/**

საიტის სტატისტიკის დირექტორია: **/var/www/<site.ge>/usage/**

საიტის ძირითადი დირექტორია: **/var/www/<site.ge>/html**

საიტის ლოგირების დირექტორია: **/var/www/<site.ge>/log**

ძირითადი სკრიპტები: **/var/www/<site.ge>/html/scripts**

Javascript –სკრიპტები: **/var/www/<site.ge>/html/scripts/js** (ან კომბინირებული*)

Css სტილები: **/var/www/<site.ge>/html/scripts/css** (ან კომბინირებული*)

საიტის Include – ჩანართები: **/var/www/<site.ge>/html/includes**

საიტის მოდულების დირექტორია: **/var/www/<site.ge>/html/modules**

საიტის იერსახე–თემების დირექტორია: **/var/www/<site.ge>/html/themes**

სიტის სხვადასხვა, არა ძირითადი ფაილების დირექტორია: **/var/www/<site.ge>/html/misc** (ამ დირექტორიაში არ შეიძლება იყოს საიტის ბირთვის საკონფიგურაციო ფაილი)

საიტის მედია რესურსების დირექტორია : **/var/www/<site.ge>/html/res**

საიტის ციფრული სურათების დირექტორია **/var/www/<site.ge>/html/res/images**

საიტის ვიდეო ფაილების დირექტორია: **/var/www/<site.ge>/html/res/videos**

საიტის აუდიო ფაილების დირექტორია: **/var/www/<site.ge>/html/res/audios**

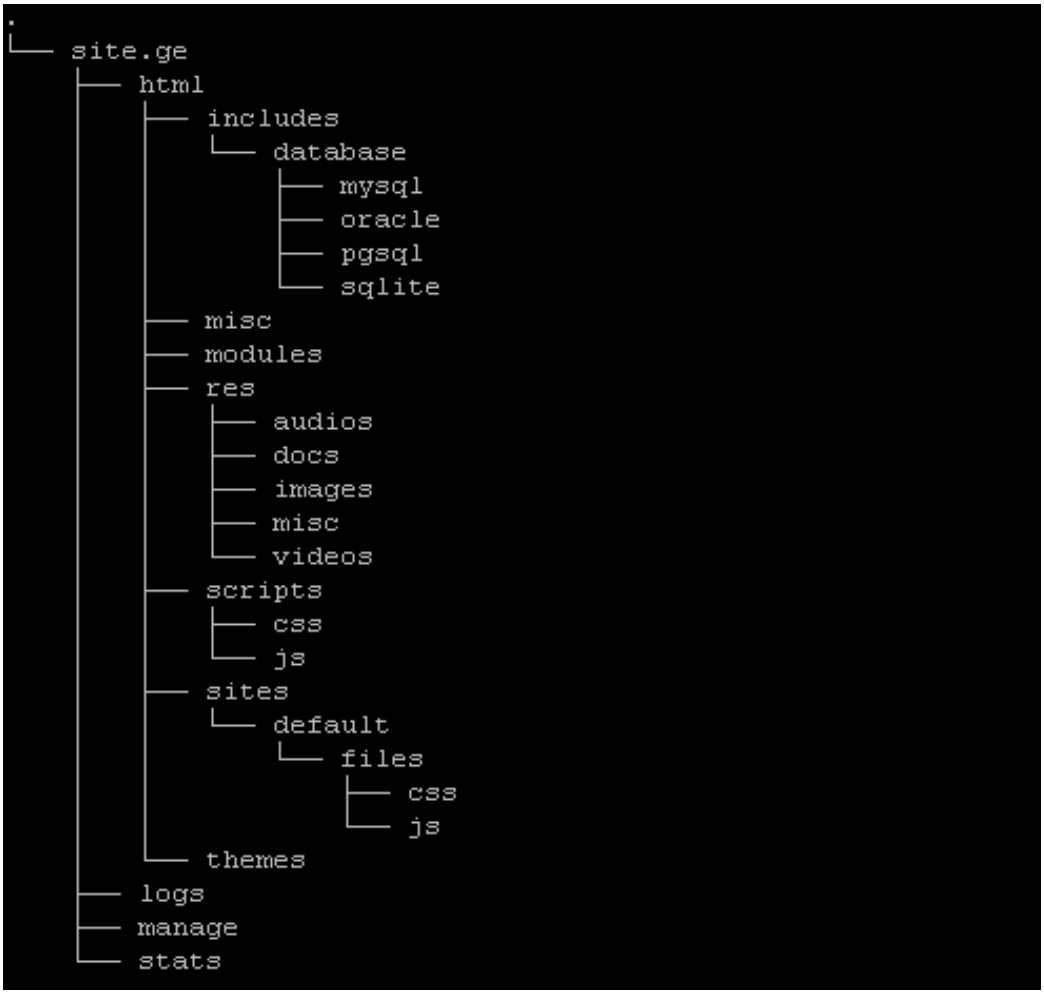
ციფრული დოკუმენტების დირექტორია: mag: *.pdf, *.doc, *.xls, etc.: **/var/www/<site.ge>/html/res/docs**

სხვადასხვა ბინარული ფაილების დირექტორია მაგ: *.zip *.bin *.exe *.msi : **/var/www/<site.ge>/html/res/misc**

საიტის დროებითი ფაილების, ან გენერირებადი სკრიპტების დირექტორია: **/var/www/<site.ge>/html/sites/default/files**

საიტის მონაცემთა ბაზების კავშირის სტრიქონის (**connection string***) დირექტორიები: **/var/www/<site.ge>/html/includes/database**

საიტის ხეს უნდა ქონდეს შემდეგი სტრუქტურული სახე:



სურ.1

⚠ საიტის ადმინისტრატორი ვალდებულია უზრუნველყოს საიტის დირექტორიების განლაგება აღნიშნული იერარქიული პრინციპით.

⚠ საიტის დეველოპერი ვალდებულია გაითვალისწინოს აღნიშნული იერარქია და შექმნას ან მოარგოს არსებული საიტი მას.

6. წვდომის უფლებები

საიტის სხვადასხვა დირექტორიაზე მოქმედებს სხვადასხვა სიღრმის წვდომის უფლება, წვდომის უფლებების აუცილებლობა განპირობებულია შემდეგი მიზეზით, რადგანაც HTTPD პროცესი გაშვებულია თავისი კუთვნილი მომხმარებლით (ნაგულისხმევად ესენია ლიმიტირებული მომხმარებლები: httpd ან apache) ვებ საიტის სკრიპტის დაუცველობის შემთხვევაში, თუ აღნშნულ HTTPD–პროცეს გააჩნია ჩაწერისა და წაკითხვის – rw უფლება დირექტორია X-ზე, მაშინ შემტევს შეუძლია გამოიყენის ხვრელი სიტის კოდში და მისი მეშვეობით შემქნას ფაილი აღნიშნულ X დირექტორიაში, რის შედეგადაც შეუძლია ტოტალური კონტროლის მოპოვება მთელ სერვერზე.

წვდომის უფლებების არასწორმა მინიჭებამ შეიძლება გამოიწვიოს შემდეგი:

- სკრიპტის ცვლადების დაუცველობის დროს phpshell*–ის შექმნა;
- ფაილის გენერირება საიტის დირექტორიაში;
- დაგენერირებული ფაილით მთლიანი საიტის მართვა;
- ფაილების წაშლა საიტის დირექტორიდან;
- ბაზის პარამეტრების ნახვა, (პაროლები მომხმარებლის სახელები) ბაზის კონტროლი;
- ბაზაში ინფორმაციის წაკითხვა არასანქცირებულად;
- ბაზის დაზიანება drop*;

6.1 წვდომის უფლებები დირექტორიებზე

დირექტორიებზე დაშვებულია შემდეგი წვდომები:

```
drwxr-xr-x   /var/var/www/site.ge
drwxr-xr-x   /var/www/site.ge/manage/
drwxr-xr-x   /var/www/site.ge/manage/
drwxr-xr-x   /var/www/site.ge/html
drwxr-xr-x   /var/www/site.ge/log
drwxr-xr-x   /var/www/site.ge/html/scripts
drwxr-xr-x   /var/www/site.ge/html/scripts/js
drwxr-xr-x   /var/www/site.ge/html/scripts/css
drwxr-xr-x   /var/www/site.ge/html/includes
drwxr-xr-x   /var/www/site.ge/html/modules
drwxr-xr-x   /var/www/site.ge/html/themes
drwxr-xr-x   /var/www/site.ge/html/misc
drwxr-xr-x   /var/www/site.ge/html/res
drwxrwxrwx   /var/www/site.ge/html/res/images
drwxrwxrwx  /var/www/site.ge/html/res/videos
drwxrwxrwx   /var/www/site.ge/html/res/audios
drwxrwxrwx   /var/www/site.ge/html/res/docs
drwxrwxrwx  /var/www/site.ge/html/res/misc
drwxrwxrwx   /var/www/site.ge/html/sites/default/files
```

```
drwxr-xr-x   /var/www/site.ge/html/includes/database
```

როგორც ჩამონათვალზე აღნიშნულია წვდომის უფლებები 777 (ყველას და ყველაფერს აქვს ჩაწერა, წაკითხვა, გაშვების უფლება) მინიჭებულია მხოლოდ, რამოდენიმე დირექტორიაზე, რომლებიც შავად არიან მონიშნულნი, ამ დირექტორიებს ჭირდებათ ასეთი წვდომის უფლებები შემდეგი მიზეზის გამო:

- ვებ საიტის ადმინისტრირების პანელიდან სურათების, ფაილების ატვირთვა;
- ვებ საიტის ადმინისტრირების პანელიდან აუდიო/ვიდეო ფაილების ატვირთვა;
- ვებ საიტის ადმინისტრირების პანელიდან დოკუმენტების ატვირთვა;
- ვებ საიტის ადმინისტრირების პანელიდან სხვადასხვა ბინარული ფაილების ატვირთვა;
- რამოდენიმე javascript ფაილის კომბინირება ერთ ფაილში;
- რამოდენიმე css ფაილის კომბინირება ერთ ფაილში;
- ატვირთვის დროს დროებითი ფაილების გენერირება;

აღნიშნულ დირექტორიებში დაუშვებელია საიტის რომელიმე სკრიპტის შესრულება, ამისტომ ეს დირექტორიები დაცული უნდა იყოს .httaccess* ფაილით, სადაც გაწერილი იქნება კონკრეტული დირექტორიისთვის კონკრეტული ფაილის ტიპის ჩაწერის და გამოძახების შესაძლებლობა.

მაგ: `var/www/site.ge/html/res/images/shell.php` არ უნდა შესრულდეს ასეთ დირექტორიებში.

⚠ საიტის ადმინისტრატორი ვალდებულია განსაზღვროს/მიანიჭოს კონკრეტული წვდომის უფლებები საიტის დირექტორიებზე.

⚠ საიტის დეველოპერი ვალდებულია გაითვალისწინოს აღნიშნული წვდომის უფლებები დირექტორიებზე, საიტის დამზადების ან მოდიფიცირების დროს.

6.2 წვდომის უფლებები ფაილებზე

წვდომის უფლებები ფაილებზე ნაგულისხმევად უნდა იყოს: `rwr-r-r` (644), საიტის შესრულებად ფაილებზე (მაგ: *.php), რადგანაც საჭიროა მხოლოდ წაკითხვის უფლება HTTPD პროცესისთვის და ვებ გვერდის ფუნქციონირებისთვის, აღნიშნული წვდომის უფლებები განხილულია , როდესაც **SuExec*** პარამეტრი არის გათიშული.

მაგ: `-rw-r--r--  /var/www/site.ge/html/index.php`

⚠ საიტის ადმინისტრატორი ვალდებულია განსაზღვროს/მიანიჭოს კონკრეტული წვდომის უფლებები საიტის ფაილებზე.

⚠ საიტის დეველოპერი ვალდებულია გაითვალისწინოს აღნიშნული წვდომის უფლებები ფაილებზე, საიტის დამზადების ან მოდიფიცირების დროს.

7. წვდომები მართვის პანელზე

საიტის ადმინისტრირების პანელზე, ან მართვის გვერდზე არასანქცირებული შეღწევა შეიძლება განხორციელდეს თუ არ არის უზრუნველყოფილი:

პუნქტები:

1. დაცვა მასიური გადასინჯვის მეთოდისგან (**bruteforce protection***);
2. **Captcha*** ავტორიზაციის დაცვა ავტომატური სკრიპტებისგან;
3. დამოუკიდებელი **VirtualHost*** მართვის პანელისთვის;

4. მკაცრი პაროლების პოლიტიკა*;
5. **https** – დაშიფრული კავშირი ავტორიზაციის დროს.

⚠ საიტის ადმინისტრატორი ვალდებულია უზრუნველყოს შემდეგი პუნქტები: 1, 3 და 5.

⚠ საიტის დეველოპერი ვალდებულია დაიცვას შემდეგი შემდეგი პუნქტები: 2, 4 და 5.

⚠ საიტის ადმინ. პანელის მომხმარებელი ვალდებულია დაიცვას პუნქტი: 4.

7.1.ვირტუალური ჰოსტი მართვის პანელისთვის

ვებ საიტის მართვის პანელისთვის აუცილებელია არსებობდეს დამოუკიდებელი VirtualHost*–ი VirtualHost–ზე უნდა განისაზღვროს მართვის პანელზე წვდომადი მომხმარებლების პარამეტრები და სხვადასხვა უსაფრთხოების საკითხები.

⚠ საიტის ადმინისტრატორი ვალდებულია უზრუნველყოს VirtualHost–ის კონფიგურაცია და განსაზღვროს წვდომის უფლებები.

⚠ საიტის დეველოპერი ვალდებულია მოარგოს საიტის მართვის პანელი VirtualHost–ს.

8. სახელმძღვანელო

8.1 პაროლების პოლიტიკა ვებ საიტებისთვის

⚠ საიტის დეველოპერი ვალდებულია უზრუნველყოს შემდეგი პუნქტები: 2, 3, 6 და 7. საიტის დეველოპერი აგრეთვე ვალდებულია მისცეს მომხმარებლებს ქვემოთ ჩამოთვლილი უფლებები და შეამოწმოს პაროლების პლოტიკით მოთხოვნილი პირობები.

⚠ საიტის მართვის პანელის ადმინისტრატორი ვალდებულია დაიცვას შემდეგი პუნქტები: 1,2,3,4 და 5.

1. პაროლები უნდა შეიცვალოს 35 დღეში ერთხელ;
2. პაროლი უნდა იყოს არანაკლებ 10 და არაუმეტეს 25 სიმბოლოსი.
3. პაროლის შერჩევის დროს გამოყენებული უნდა იყოს: მაღალი და დაბალი რეგისტრის ასოები რიცხვები და სიმბოლოები. კერძოდ ძლიერი პაროლი უნდა შეიცავდეს მინ: 4 ციფრს, 4 მაღალი რეგისტრის ასოებს, 4 დაბალი რეგისტრის ასოებს, 4 სიმბოლოს.
4. პაროლის შერჩევის დროს დაუშვებელია Unicode ტიპის სიმბოლოები გამოყენება;
5. **პაროლის შერჩევის დროს მნიშვნელობა არ აქვს მესამე პუნქტის თანმიმდევრობას, მაგრამ, სიმბოლოების შერჩევის დროს გამოყენებული უნდა იყოს მხოლოდ შემდეგი:**
   - 5.1 მაღალი რეგისტრის ასოები: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
   - 5.2 დაბალი რეგისტრის ასოები: a b c d e f g h i j k l m n o p q r s t u v w x y z
   - 5.3 ციფრები: 1 2 3 4 5 6 7 8 9 0
   - 5.4 სიმბოლოები: ~ ! @ # $ % ^ & * ( ) _ + { } [ ] : ” | ; ’ \ < > ? , . /
6. საიტის ადმინისტრატორის მოვალეობის შემსრულებლის არსებობის შემთხვევაში უნდა გაუქმდეს არსებული პაროლი, დაგენერირდეს ახალი პაროლი აღნშნული პირისთვის და განისაზღვროს მოქმედების ვადა.
7. ვებ დეველოპერმა უნდა უზრუნველყოს ძლიერი შიფრირების ალგორითმებით პაროლების შიფრაცია ბაზაში და შეინახოს დშიფრული სახით, საქართველოს იუსტიციი სამინისტროს მოთხოვნით ეს ალგორითმი უნდა იყოს - SHA1.

მაგ:
```
mysql> INSERT INTO site.ge_users VALUES ('sitemanager1',SHA1('secretpassword') );
```

9. ტერმინოლოგია და განმარტება

1.Upload Code injection - შეტევა, რომლის დროსაც ხორციელდება სურათის გაფართოების ფაილის ატვირთვა მაგ: Logo.jpg სინამდვილეში, ამ ფაილში წერია შესრულებადი კოდი, ასევე შეტევა როდესაც დაუცველი საიტის კოდი გაძლევთ საშუალებას ატვირთოდ პირდაპირ შესრულებადი კოდის გაფართოების ფაილი, მაგ: *.php.

phpshell - ეს არის შესრულებადი კოდი ვებ სერვერზე, რომელსაც შეუძლია ვებ სერვერის მართვა და სისტემური ბრძანებების გამოძახება, მაგ: poweroff, ასევე შესაძლებელია ფაილებზე და დირექტორიებზე წვდომა მისი მეშვეობით.

drop - ეს ბრძანება გამოიყენება მონაცამთა ბაზის ცხირლის წასაშლელად, მაგ: mysql> drop table sitenews; ან მთელი მონაცემთა ბაზის წასაშლელად.

httaccess - ვებ საიტის კონფიგურაციის ფაილი, რომელშიც იწერება წესები კონკრეტული დირექტორიისთვის ან მთელი საიტისთვის, მაგალითად რესურსის ან ბმულის გადამისამართება სხვა ბმულზე, ფაილების გაფართოების განსაზღვრა, „ბმულის გადაწერის“ მეთოდების გამოყენება: (http://site.ge/1 > http://site.ge/2), და სხვა მრავალი წესის დადგენა.

SuExec – ეს პარამეტრი გამოიყენება სხვადასხვა ტიპის ჰოსტინგ არქირექტურაში, როდესაც აღნიშნული პარამეტრი ჩართულია, http პროცეს გააჩნია საკუთრების უფლება ნებისმიერ ფაილზე თავის სამუშაო დირექტორიაში, მაგ: -rw-r--r-- admin admin test.htlml ამ დროს http პროცესი გაშვებულია admin მომხმარებლის უფლებით.

bruteforce protection – დაცვა გადასინჯვის მეთოდისგან, როდესაც შემტევი ცდილობს მომხმარებლის სახელის ან პაროლის გამოცნობას ავტომატური გადასინჯვის მეთოდით.

connection string – კავშირის სტრიქონი, ამ სტრიქონში წინასწარ არის გაწერილი მონაცემთა ბაზასთან დაკავშირების პარამეტრები, ჰოსტის მისამართი, ბაზის სახელი, მომხმარებლის სახელი და პაროლი.

Captcha – ავტორიზაციის დაცვის მექანიზმი, ძირითადათ გავრცელებულია დახატული სურათების სახით, სადაც მომხმარებელმა უნდა ამოიცნოს დახტული ციფრი ან სიმბოლო და შეიყვანოს განკუთვნუილ ველში. გამოიყენება სპამ რობოტებთან და ავტომატურ სკრიპტებთან საბრძოლველად.

VirtualHost – ვირტუალური საიტი, გამოიყენება ერთ ფიზიკურ სერვერზე რამოდენიმე საიტის განსათავსებლად, მაგ: example.ge და site.ge შეიძლება განთავსებული იყოს ერთ ვებ სერვერზე.