EPIC
Institute of Technology
Powered by epam

Security

Course: Real-Time Backend

Lecturer: Gleb Lobanov

June, 2024

EPIC
Institute of Technology
Powered by epam

Contents

EPIC
Institute of Technology
Powered by <epam>

01

Why do we need security?

EPIC
Institute of Technology
Powered by epam

Main purposes

1) Protection of user data from unauthorized access and theft.
2) Ensuring the correct operation of the web application, preventing failures and downtimes.
3) Protection of the company's infrastructure and resources from malicious impacts.

EPIC
Institute of Technology
Powered by epam

02

CIA Triad

EPIC
Institute of Tech
Powered by <epam>

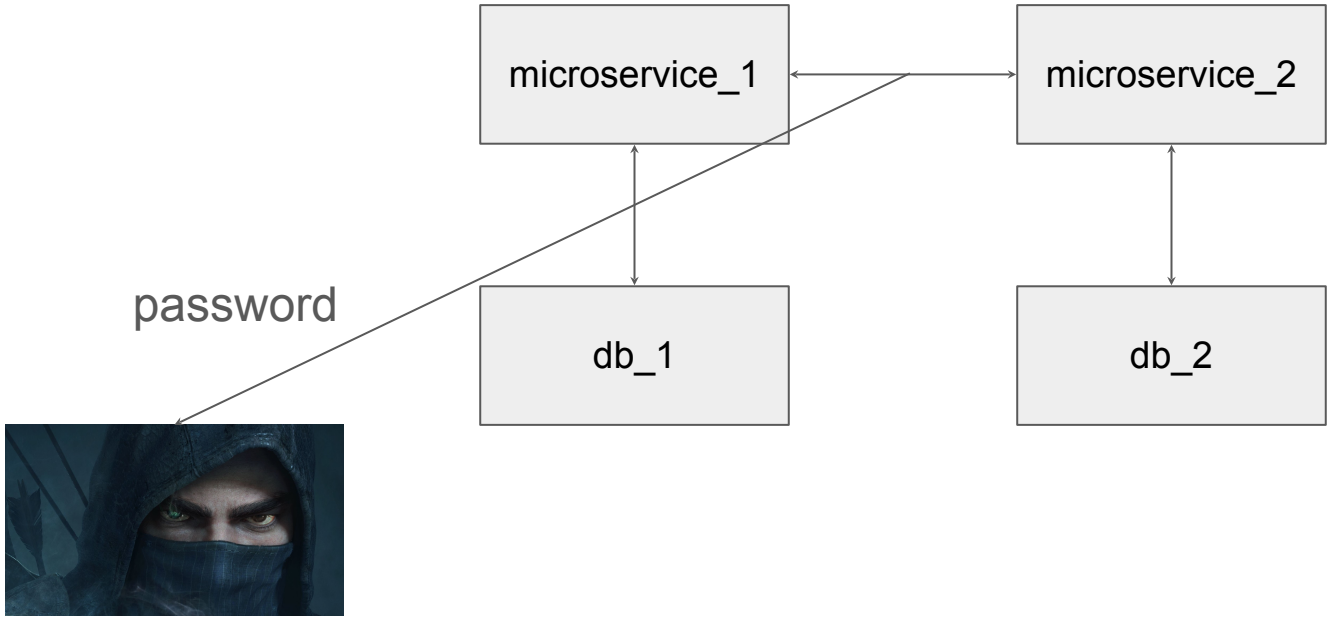
EPIC
Institute of Technology
Powered by epam

Main purposes

1) Confidentiality — ensures that only authorized user/system/ resource can view, access, change, or otherwise use data.
2) Integrity — ensures that the system and information is accurate and correct.
3) Availability — ensures that systems, information, and services are available the vast majority of time.

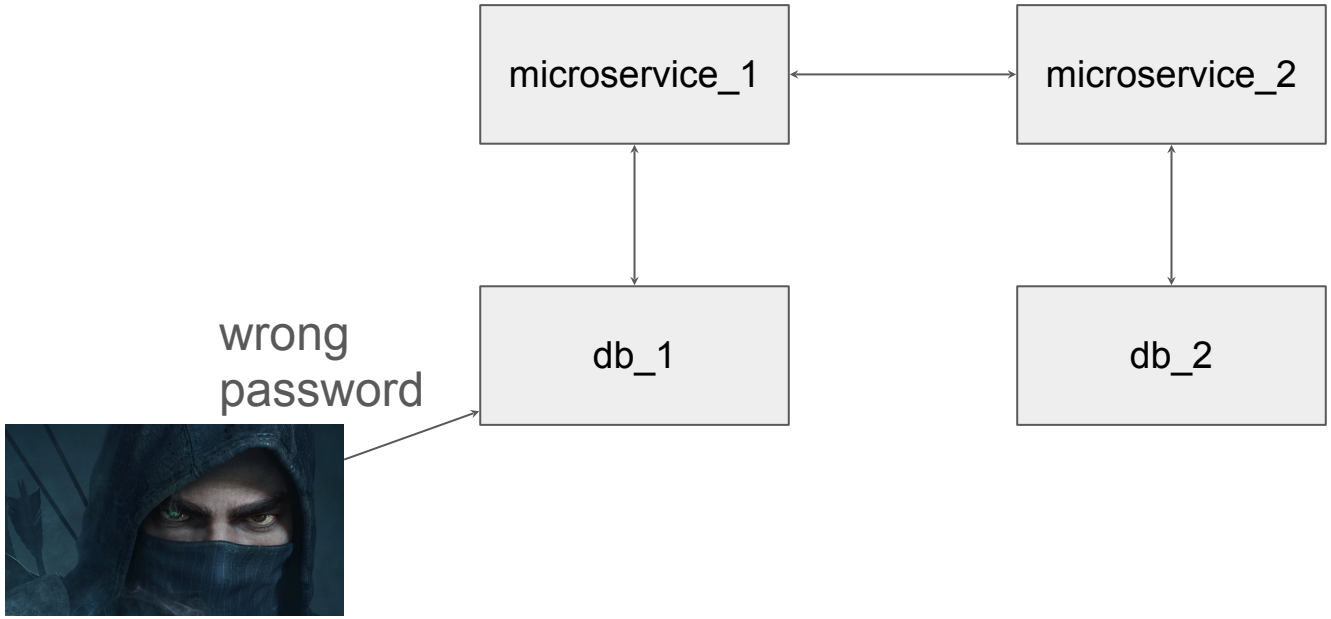
EPIC
Institute of Technology
Powered by <epam>

Confidentiality



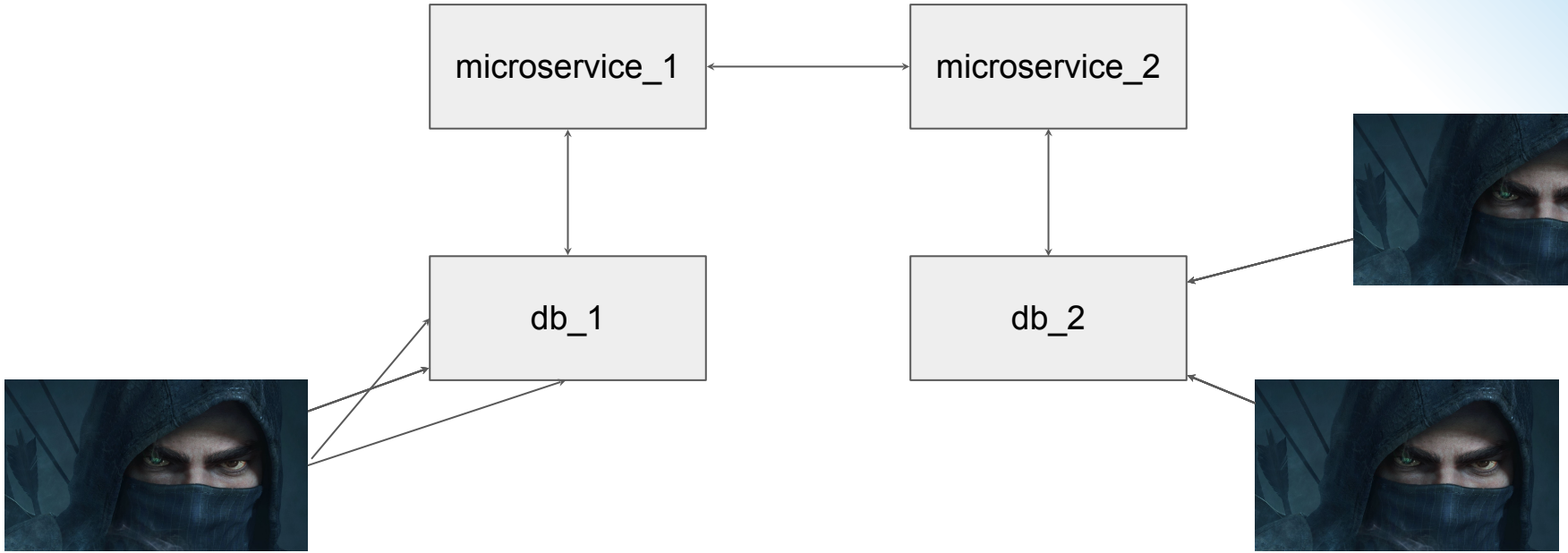
EPIC
Institute of Technology
Powered by epam

Integrity



EPIC
Institute of Technology
Powered by epam

Availability



EPIC
Institute of Technology
Powered by <epam>

03

The most known examples

EPIC Institute of Technology
Powered by epam

SQL Injection: Target (2013)

Credit card companies, banks and retailers say that victims of any fraud resulting from the theft of their payment card data bear "zero liability" and will be credited for fraudulent purchases made on their accounts.

"Our rules say five days, but most consumers get (their money) back within 24 hours," Visa spokeswoman Rosetta Jones said.

Yet consumer advocates said that any debit card fraud could result in money being drained from a bank, mutual fund or other cash account at a time when those funds were really needed.

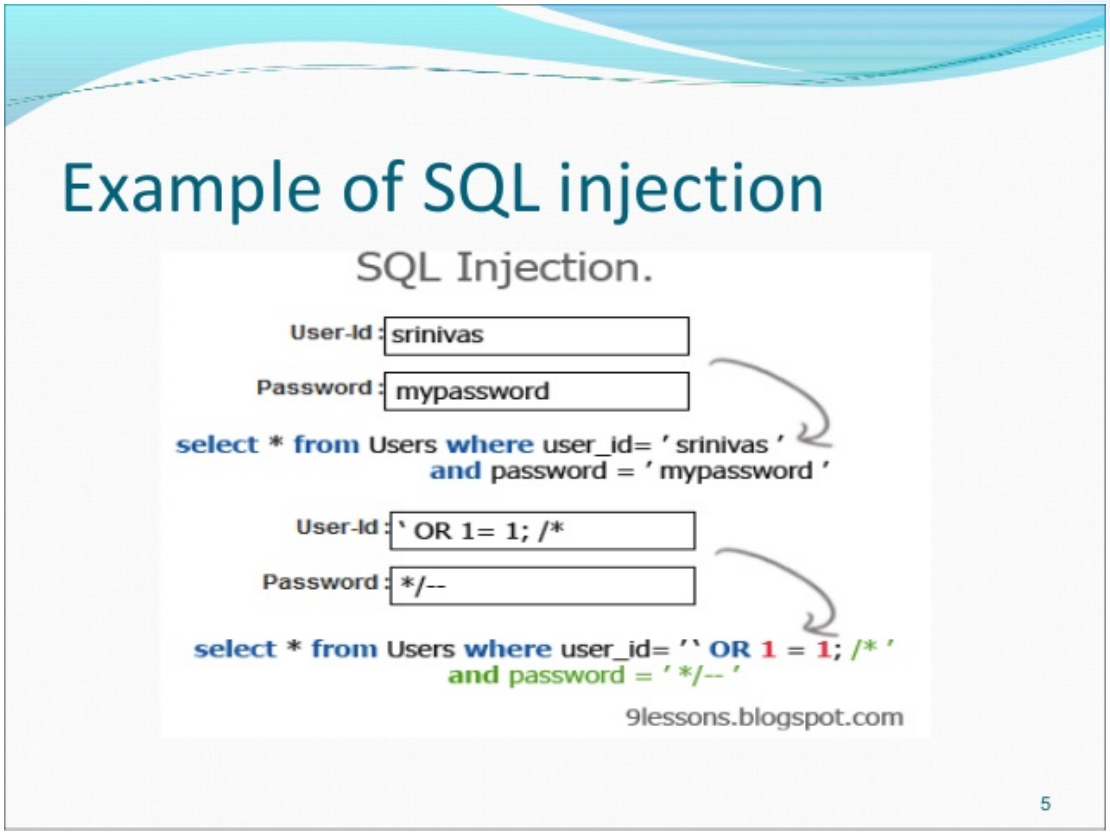
EPIC Institute of Technology
Powered by epam

SQL Injection: Target (2013)

The Target data breach of 2013 is considered to be one of the largest data breaches in the history of the United States. In December of 2013, credit card numbers of almost 40 million customers were stolen from 2000 Target stores around the country by accessing data on point of sale (POS) systems. A Point-of-Sale system or POS is the place where the customer makes the payment for the products or services at a store. On the 10th of January 2014, Target announced that Personally Identifiable Information (PII) data i.e. names, phone numbers, addresses, and email addresses of up to 70 million customers were stolen. In both types of data stolen, there was an overlap of 12 million people. So, in total, around 98 million people were affected. In estimation, almost 11 GB of data was stolen. The stolen data of the customers was available on online black-market forums known as “card shops” for sale. The U.S Governing body i.e. Senate Committee on Commerce concluded in March 2014 that Target had missed opportunities to prevent the breach resulting in such catastrophic outcomes. The management of Target reported that the breach cost them over $61 million. It was also reported that

EPIC
Institute of Technology
Powered by epam

SQL Injection



EPIC Institute of Technology
Powered by epam

XSS: MySpace (2005)

The next step was to simply instruct the Web browser to load a MySpace URL that would automatically invite Samy as a friend, and later add him as a "hero" to the visitor's own profile page. To do this without a user's knowledge, the code utilized XMLHTTPRequest – a JavaScript object used in AJAX, or Web 2.0, applications such as Google Maps.

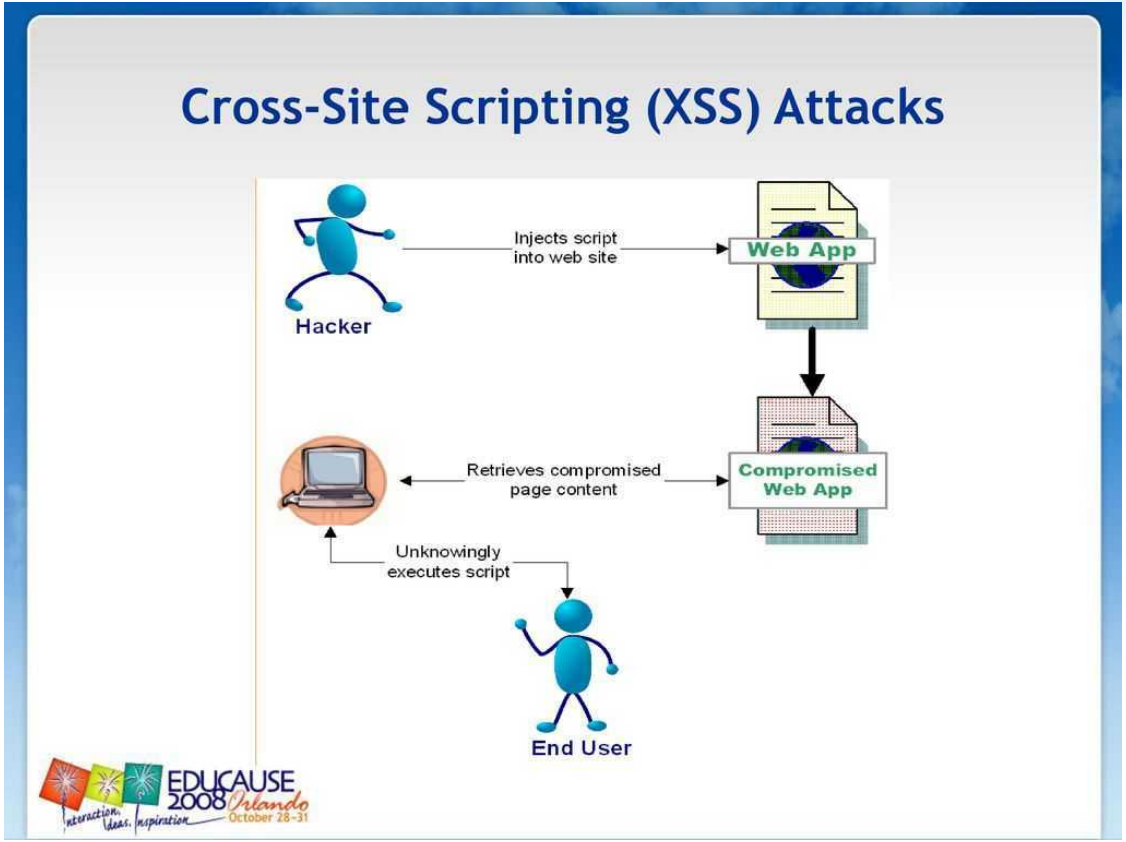
Taking the hack even further, Samy realized that he could simply insert the entire script into the visiting user's profile, creating a replicating worm. "So if 5 people viewed my profile, that's 5 new friends. If 5 people viewed each of their profiles, that's 25 more new friends," Samy explained.

It didn't take long for friend requests to start rolling in – first in the hundreds, then thousands. By 9:30pm that night, requests topped one million and continued arriving at a rate of 1,000 every few seconds. Less than an hour later, MySpace was taken offline while the worm was removed from all user profiles.

Samy says his intentions weren't malicious, but expressed concern that MySpace, which was purchased by News Corp. in July for $580 million, wouldn't see it that way. Company officials have not contacted him, but his account was deleted.

EPIC
Institute of Technology
Powered by <epam>

XSS

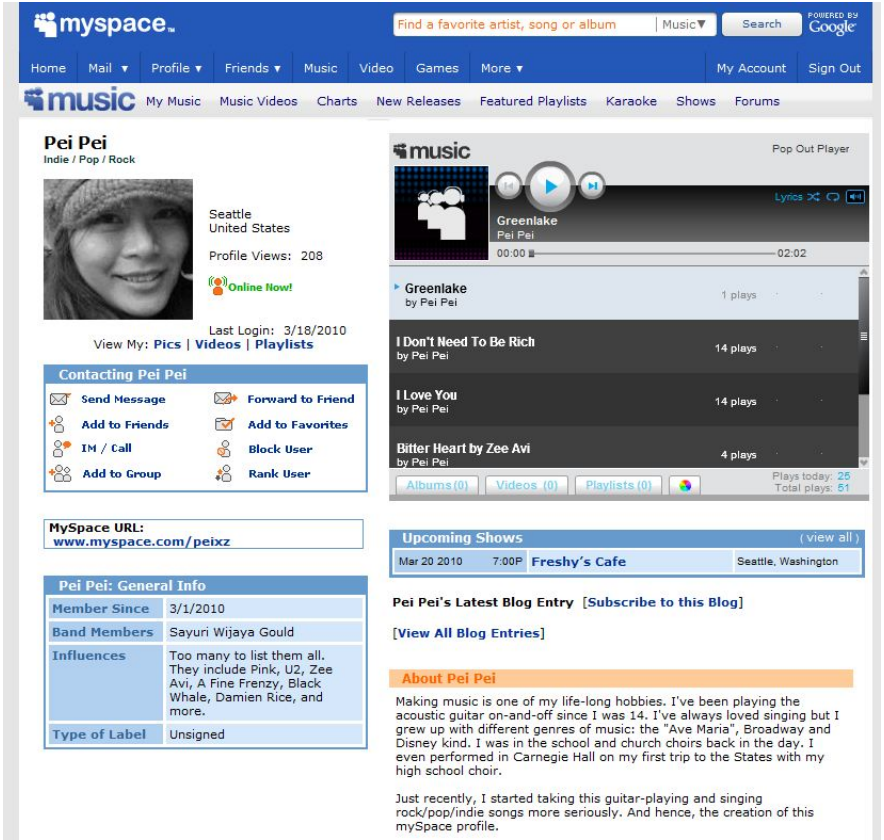


EPIC
Institute of Technology
Powered by epam

XSS

EPIC
Institute of Technology
Powered by <epam>

MySpace



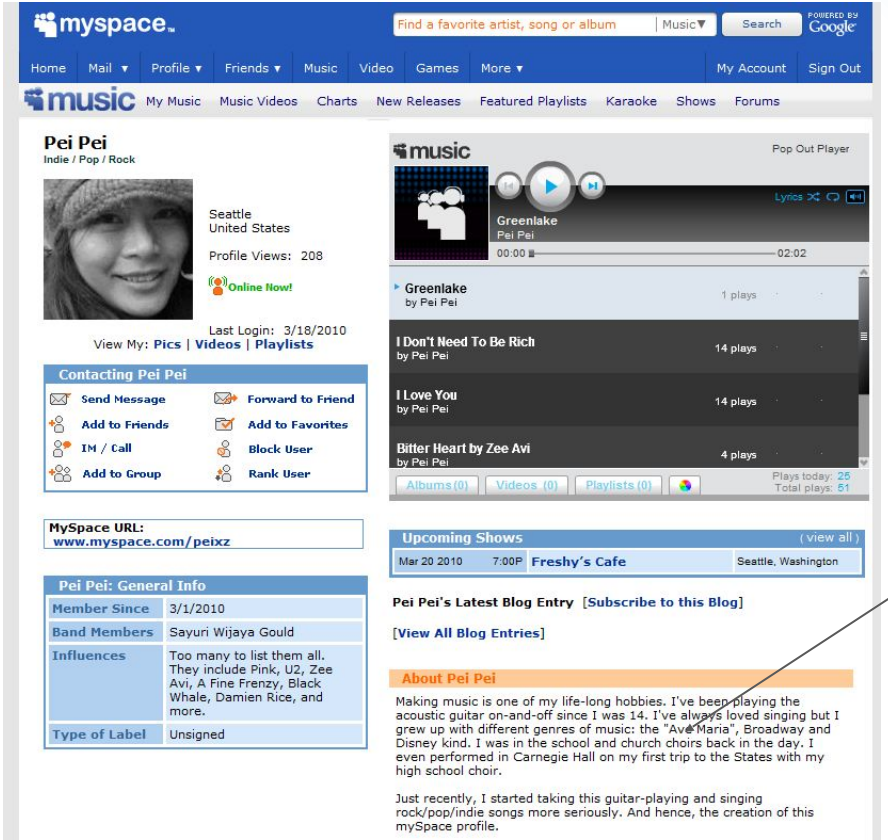
EPIC
Institute of Technology
Powered by epam

Worm

```
<script type="text/javascript">
window.onload = function() {
    if (!document.getElementById('samy')) {
        var i = document.createElement('iframe');
        i.style.display = 'none';
        i.src = 'http://myspace.com/samy';
        i.id = 'samy';
        document.body.appendChild(i);
    }
};
</script>
```

EPIC
Institute of Technology
Powered by <epam>

MySpace



worm

EPIC
Institute of Technology
Powered by epam

DDOS: DYN(2016)

DDoS attacks on Dyn

Article Talk

From Wikipedia, the free encyclopedia

On October 21, 2016, three consecutive distributed denial-of-service attacks were launched against the Domain Name System (DNS) provider Dyn. The attack caused major Internet platforms and services to be unavailable to large swathes of users in Europe and North America.[3][4] The groups Anonymous and New World Hackers claimed responsibility for the attack, but scant evidence was provided.[5]

As a DNS provider, Dyn provides to end-users the service of mapping an Internet domain name—when, for instance, entered into a web browser—to its corresponding IP address. The distributed denial-of-service (DDoS) attack was accomplished through numerous DNS lookup requests from tens of millions of IP addresses.[6] The activities are believed to have been executed through a botnet consisting of many Internet-connected devices—such as printers, IP cameras, residential gateways and baby monitors—that had been infected with the Mirai malware.

EPIC
Institute of Technology
Powered by epam

MitM: GMail(2011)

Google Security Blog

The latest news and insights from Google on security and safety on the Internet

An update on attempted man-in-the-middle attacks

August 29, 2011

Posted by Heather Adkins, Information Security Manager

Today we received reports of attempted SSL man-in-the-middle (MITM) attacks against Google users, whereby someone tried to get between them and encrypted Google services. The people affected were primarily located in Iran. The attacker used a fraudulent SSL certificate issued by DigiNotar, a root certificate authority that should not issue certificates for Google (and has since revoked it).

Google Chrome users were protected from this attack because Chrome was able to detect the fraudulent certificate.

EPIC
Institute of Technology
Powered by epam

IDOR: Uber(2016)

As Uber's CEO, it's my job to set our course for the future, which begins with building a company that every Uber employee, partner and customer can be proud of. For that to happen, we have to be honest and transparent as we work to repair our past mistakes.

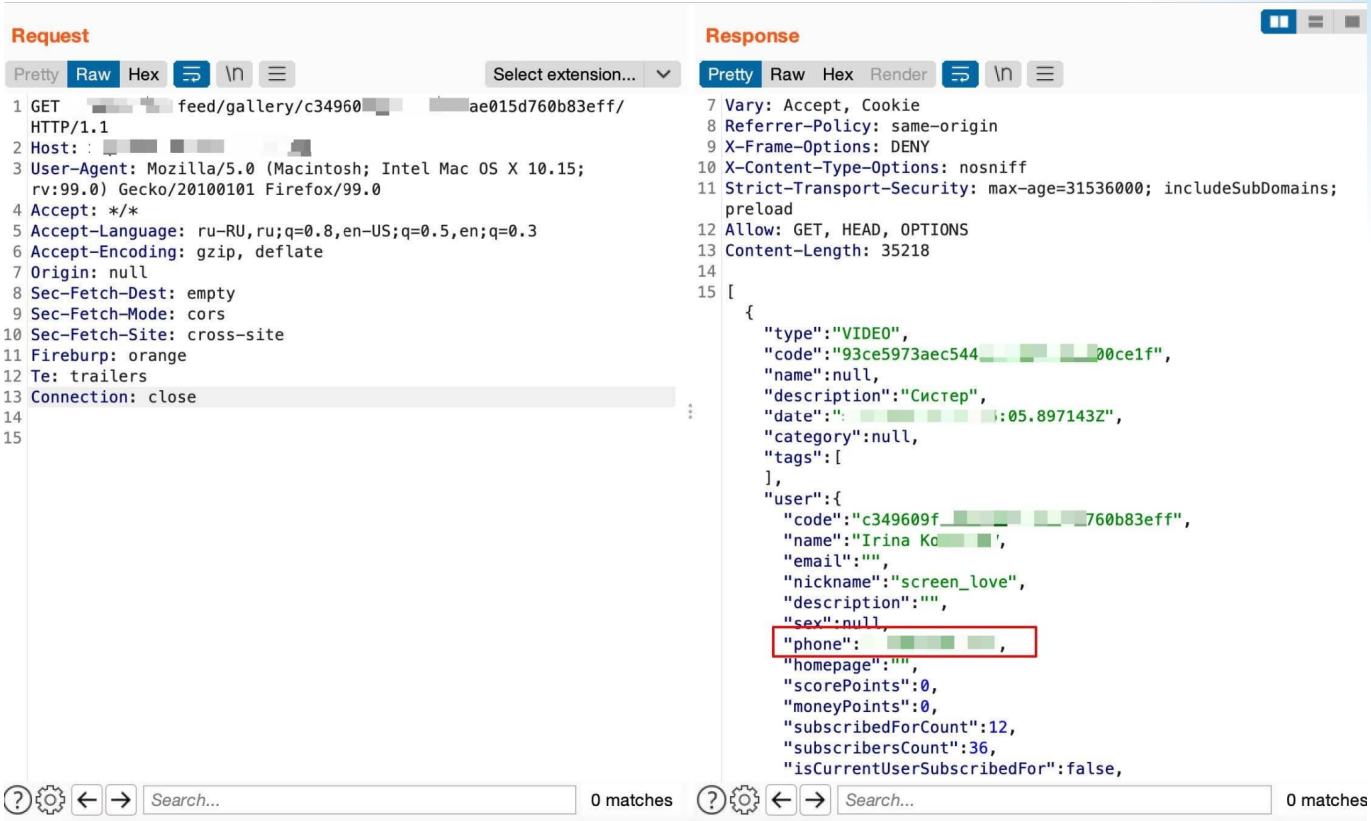
I recently learned that in late 2016 we became aware that two individuals outside the company had inappropriately accessed user data stored on a third-party cloud-based service that we use. The incident did not breach our corporate systems or infrastructure.

Our outside forensics experts have not seen any indication that trip location history, credit card numbers, bank account numbers, Social Security numbers or dates of birth were downloaded. However, the individuals were able to download files containing a significant amount of other information, including:

- The names and driver's license numbers of around 600,000 drivers in the United States. Drivers can learn more **here**.
- Some personal information of 57 million Uber users around the world, including the drivers described above. This information included names, email addresses and mobile phone numbers. Riders can learn more here.

EPIC
Institute of Technology
Powered by <epam>

simple Get



EPIC
Institute of Technology
Powered by <epam>

Real situation

`https://support.uber.com/user/12345`

`https://support.uber.com/user/67890`

EPIC Institute of Technology
Powered by epam

Social: Twitter(2020)

On July 14 and 15, 2020, the Hackers attacked Twitter.[26] The Twitter Hack happened in three phases: (1) social engineering attacks to gain access to Twitter's network; (2) taking over accounts with desirable usernames (or "handles") and selling access to them; and (3) taking over dozens of high-profile Twitter accounts and trying to trick people into sending the Hackers bitcoin. All this happened in roughly 24 hours.

EPIC
Institute of Technology
Powered by epam

Social: Twitter(2020)

Hello, i work here, give me password

I forgot it

EPIC
Institute of Technology
Powered by epam

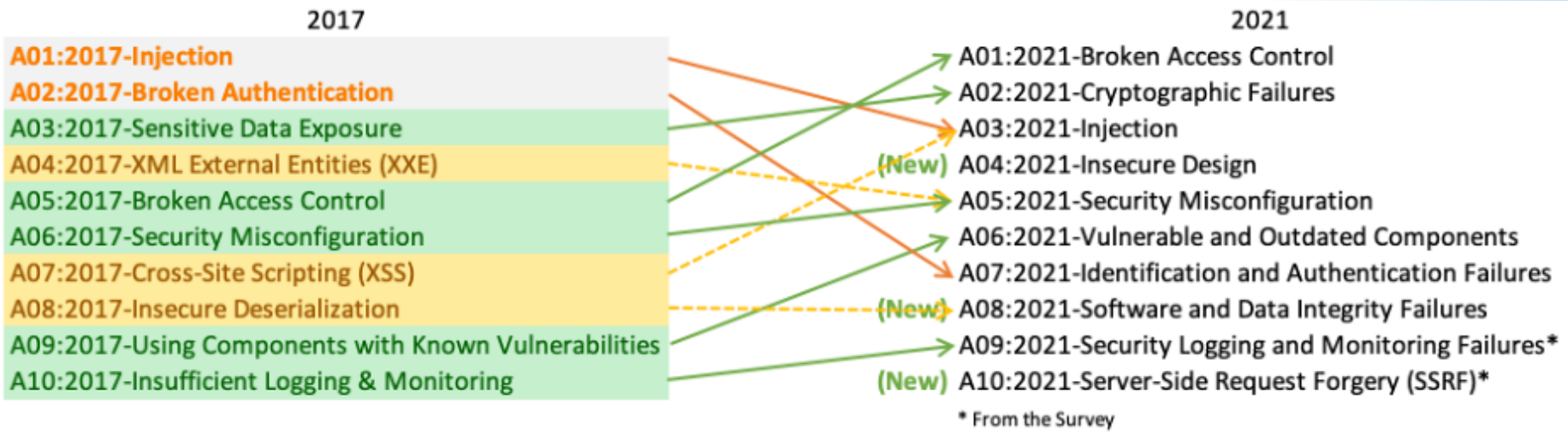
Social: Twitter(2020)

sure, the password is “ ”

twitter

EPIC Institute of Technology
Powered by epam

Comparison



owasp

EPIC Institute of Technology
Powered by epam

Comparison

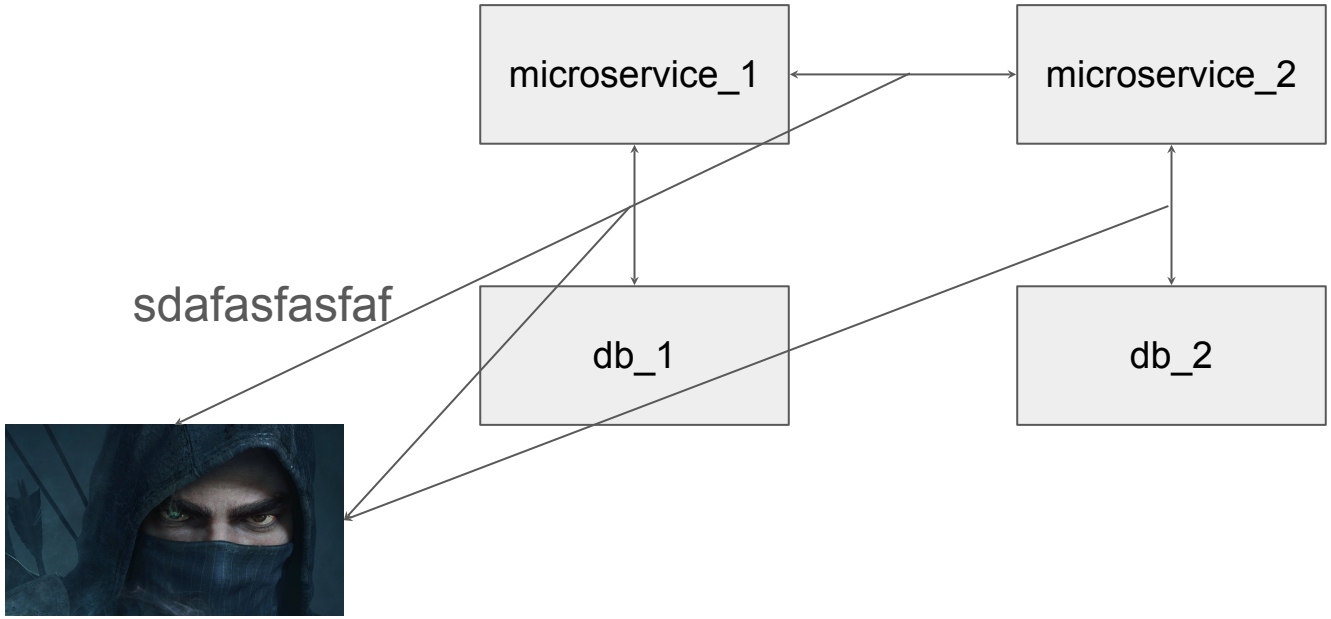
	A	B	C	D	E	F	G	H
1	OWASP Top Ten	2003	2004	2007	2010	2013	2017 RC1	2017 RC2
2	Unvalidated Input	A1	A1[9]	✗	✗	✗	✗	✗
3	Buffer Overflows	A5	A5	✗	✗	✗	✗	✗
4	Denial of Service	✗	A9[2]	✗	✗	✗	✗	✗
5	Injection	A6	A6[3]	A2	A1[10]	A1	A1	A1
6	Cross Site Scripting (XSS)	A4	A4	A1	A2	A3	A3	A7
7	Broken Authentication and Session Management	A3	A3	A7	A3	A2	A2	A2
8	Insecure Direct Object Reference	✗	A2	A4[11]	A4	A4	A4[20]	A5[20]
9	Cross Site Request Forgery (CSRF)	✗	✗	A5	A5	A8	A8	✗
10	Security Misconfiguration	A10	A10[3][5]	✗	A6	A5	A5	A6
11	Broken Access Control	A2	A2[1]	A10[13]	A8	A7[16]	A4	A5
12	Insufficient Attack Protection	✗	✗	✗	✗	✗	A7	✗
13	Unvalidated Redirects and Forwards	✗	✗	✗	A10	A10	✗	✗
14	Information Leakage and Improper Error Handling	A7	A7[14][4]	A6	A6[8]	✗	✗	✗
15	Malicious File Execution	✗	✗	A3	A6[8]	✗	✗	✗
16	Sensitive Data Exposure	A8	A8[6][5]	A8	A7	A6[17]	A6	A3
17	Insecure Communications	✗	A10	A9[7]	A9	✗	✗	✗
18	Remote Administration Flaws	A9	✗	✗	✗	✗	✗	✗
19	Using Known Vulnerable Components	✗	✗	✗	✗	A9 [18][19]	A9	A9
20	Unprotected APIs	✗	✗	✗	✗	✗	A10	✗

04

How to prevent some of them?

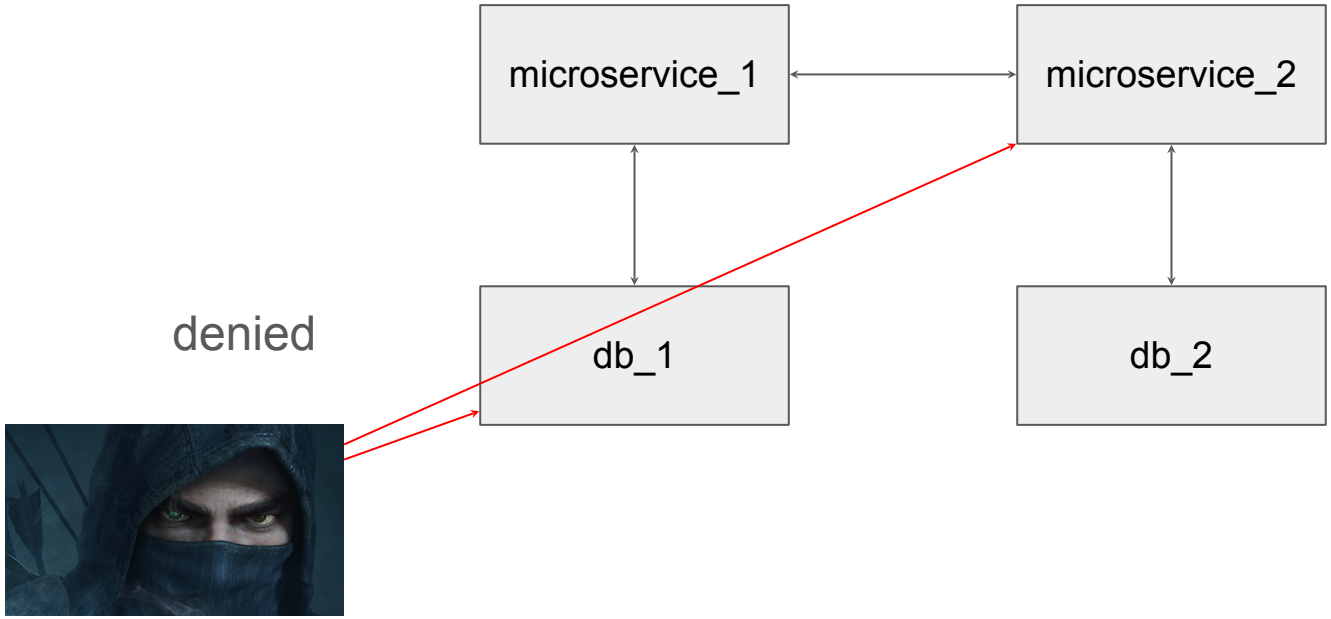
EPIC
Institute of Technology
Powered by epam

Cryptography



EPIC Institute of Technology
Powered by epam

Access Control(1 way)

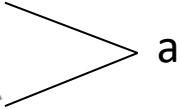


EPIC Institute of Technology
Powered by <epam>

Access Control(2 way)

`https://support.uber.com/user/12345`

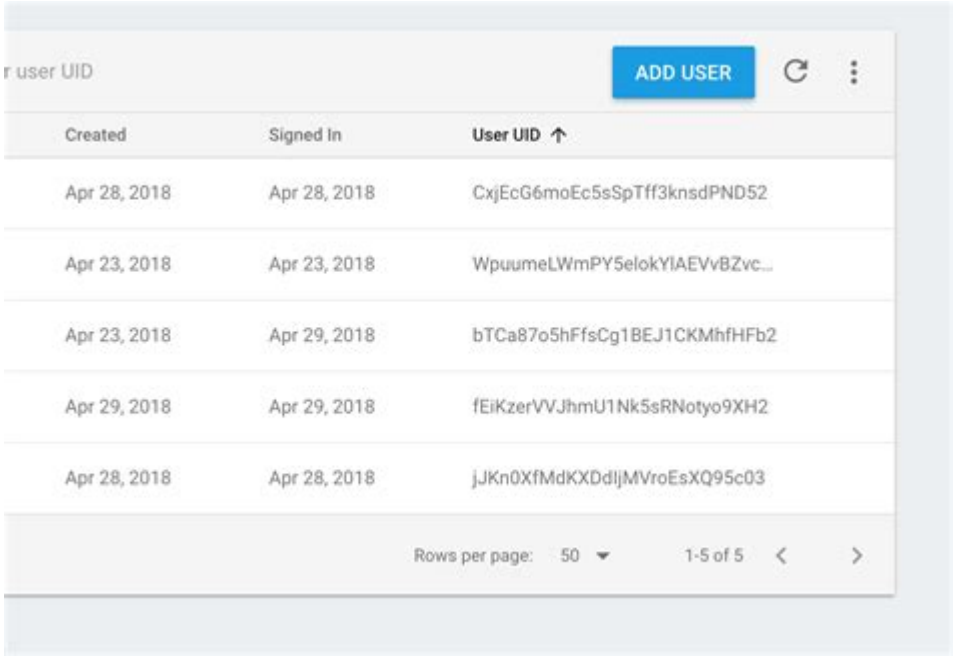
`https://support.uber.com/user/67890`



auth support_1

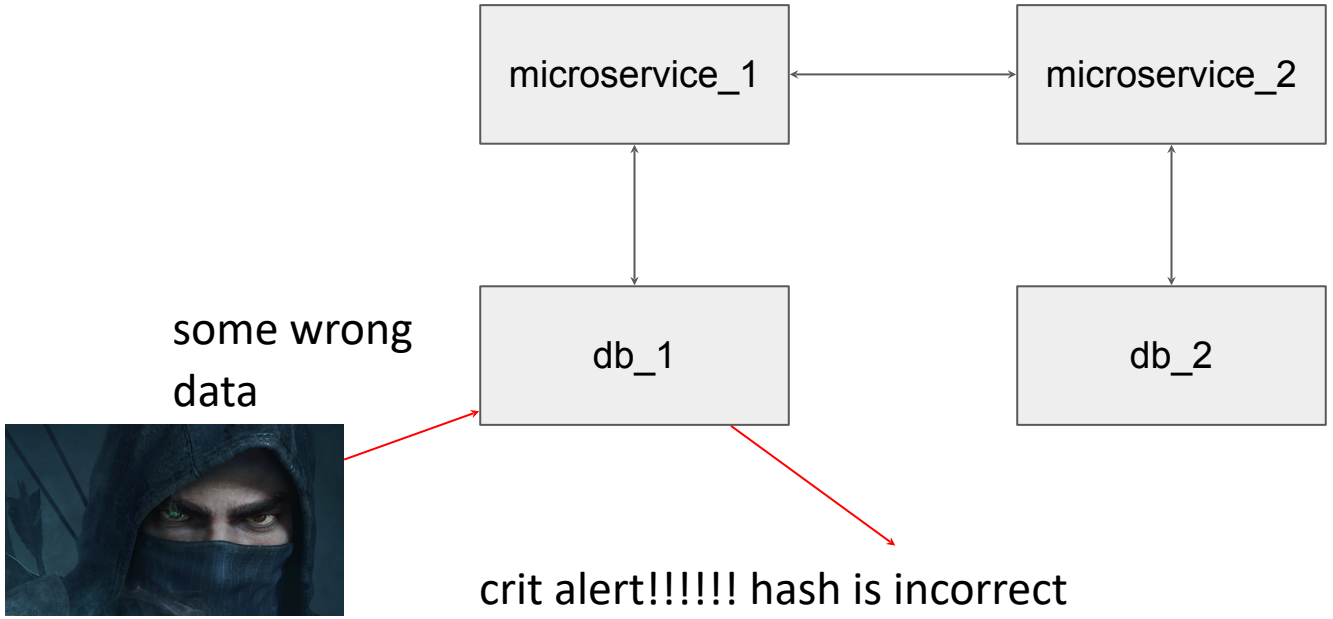
EPIC
Institute of Technology
Powered by <epam>

UID



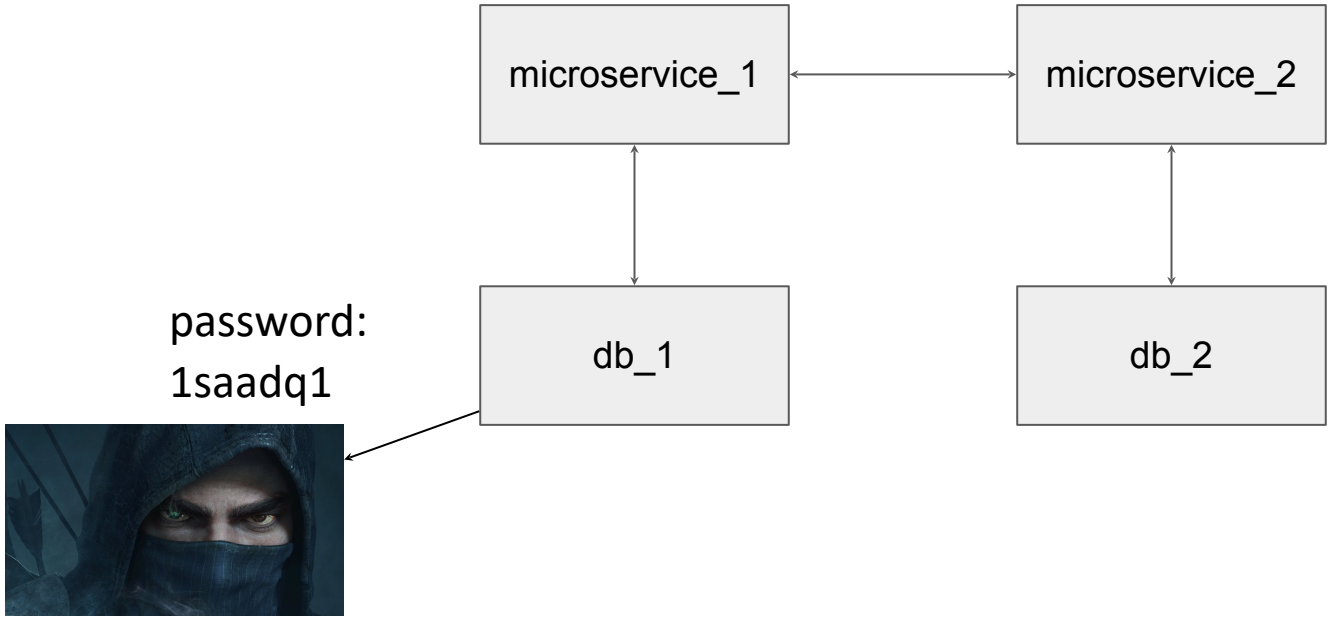
EPIC Institute of Technology
Powered by epam

Hashing(save hash of data)



EPIC
Institute of Technology
Powered by epam

Hashing of info



EPIC Institute of Technology
Powered by epam

Bad architecture

```
$name   = $_POST['name'];
$query  = "SELECT phone_number FROM users WHERE name = '$name'";
$result = mysql_query($query);
```

Get register{name, query}

EPIC
Institute of Technology
Powered by epam

Injection

Alex

```
SELECT phone_number FROM users WHERE name = 'Alex'
```

Mc'Donalds

```
SELECT phone_number FROM users WHERE name = 'Mc'Donalds'
```

Joe'; DROP TABLE users; --

```
SELECT phone_number FROM users WHERE name = 'Joe'; DROP TABLE users; --'
```

EPIC
Institute of Technology
Powered by epam

Also Injection

```
<div class="post">
    <p class="meta">
        Posted by <?php echo $post['username']; ?>
        on <?php echo date('F j, H:i', $post['date']); ?>
    </p>
    <p class="body">
        <?php echo $post['body']; ?>
    </p>
</div>
```

EPIC
Institute of Technology
Powered by epam

Also Injection

```
<div class="post">
    <p class="meta">
        Posted by JackTR
        on July 18, 12:56
    </p>
    <p class="body">
        <script src="http://evil.com/dangerous.js"
            type="text/javascript" charset="utf-8"></script>
    </p>
</div>
```

EPIC
Institute of Technology
Powered by epam

Escape character

```
$name   = $_POST['name'];
$name   = mysql_real_escape_string($name);
$query  = "SELECT phone_number FROM users WHERE name = '$name'";
$result = mysql_query($query);
```

EPIC
Institute of Technology
Powered by <epam>

Escape character

Joe'; DROP TABLE users; --

```
SELECT phone_number FROM users WHERE name = 'Joe\'; DROP TABLE users; --'
```

EPIC
Institute of Technology
Powered by epam

Escape character

```
<div class="post">
    <p class="meta">
        Posted by <?php echo htmlspecialchars($post['username']); ?>
        on <?php echo date('F j, H:i', $post['date']); ?>
    </p>
    <p class="body">
        <?php echo htmlspecialchars($post['body']); ?>
    </p>
</div>
```

EPIC
Institute of Technology
Powered by epam

Social

Dont give your info to anybody

EPIC
Institute of Technology
Powered by epam

Social

Hello, i work here, give me password,

i forget it

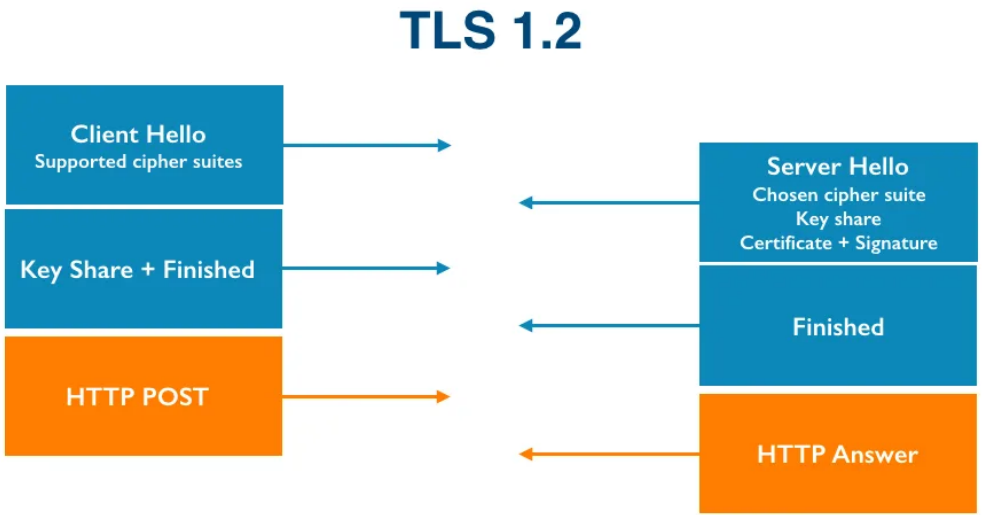
EPIC
Institute of Technology
Powered by epam

Social

No, you are a scammer

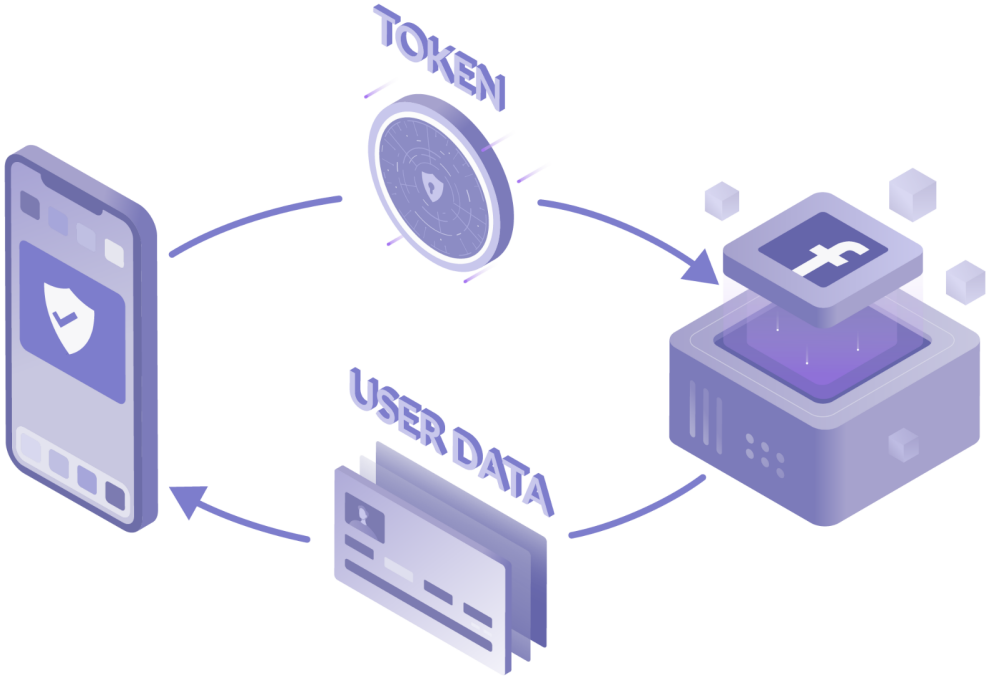
EPIC
Institute of Technology
Powered by <epam>

Sertificates



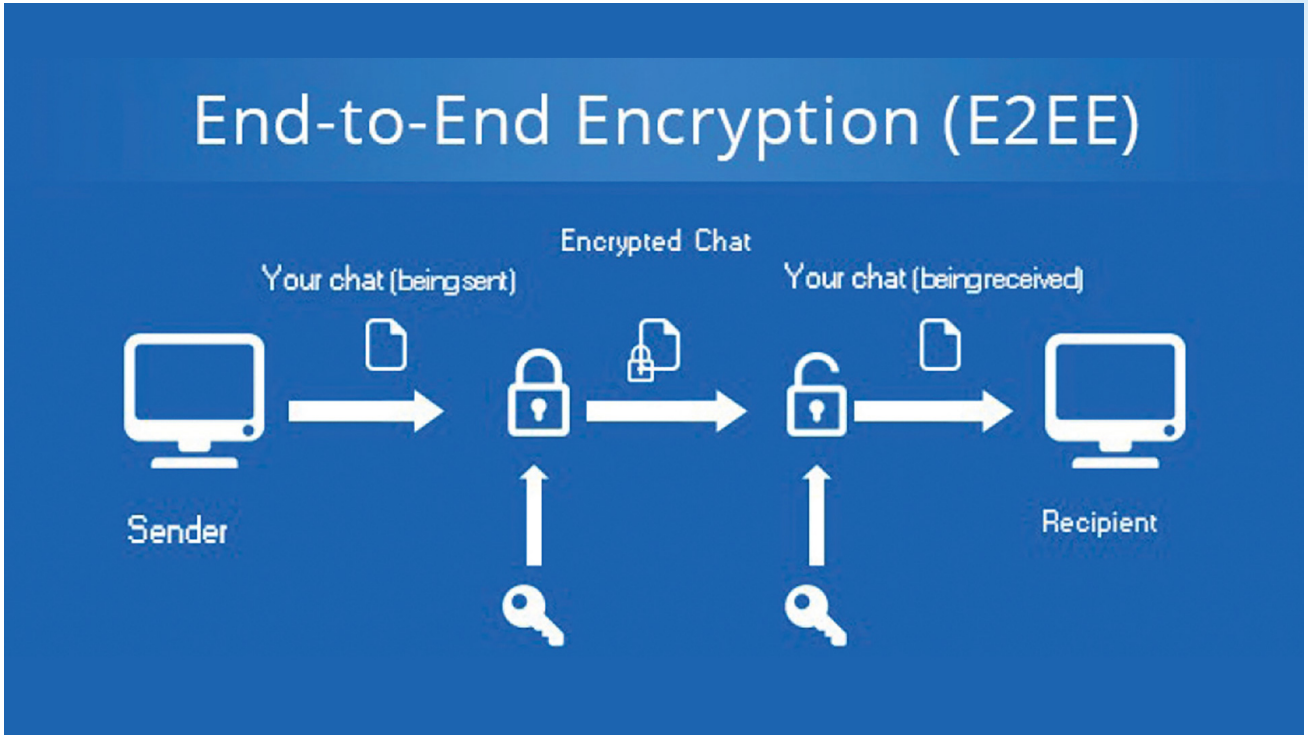
EPIC
Institute of Technology
Powered by <epam>

Oauth



EPIC
Institute of Technology
Powered by <epam>

E2EE



EPIC
Institute of Technology
Powered by <epam>

Dependency-Check

Introduction

The OWASP Top 10 2013 contains a new entry: A9-Using Components with Known Vulnerabilities. Dependency Check can currently be used to scan applications (and their dependent libraries) to identify any known vulnerable components.

The problem with using known vulnerable components was described very well in a paper by Jeff Williams and Arshan Dabirsiaghi titled, "Unfortunate Reality of Insecure Libraries". The gist of the paper is that we as a development community include third party libraries in our applications that contain well known published vulnerabilities (such as those at the National Vulnerability Database).

EPIC
Institute of Technology
Powered by epam

05

How to find them?

EPIC
Institute of Technology
Powered by <epam>

OWASP ZAP

ZAP (short for Zed Attack Proxy), formerly known as OWASP ZAP, is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.

It has been one of the most active Open Worldwide Application Security Project (OWASP) projects[3] and has been given Flagship status.[4]

When used as a proxy server it allows the user to manipulate all of the traffic that passes through it, including traffic using HTTPS.

It can also run in a daemon mode which is then controlled via a REST API.

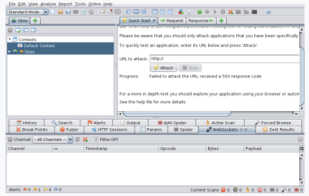
ZAP was added to the ThoughtWorks Technology Radar on May 30, 2015 in the Trial ring.[5]

ZAP was originally forked from Paros, another pentesting proxy. Simon Bennetts, the project lead, stated in 2014 that only 20% of ZAP's source code was still from Paros.[6]

As of August 1, 2023, the ZAP development team announced that ZAP was leaving the OWASP Foundation to join The Software Security Project, as a founding project [7][8] and henceforth will be simply called **ZAP**.

The OWASP Foundation announced this departure on the following day.[9]

ZAP

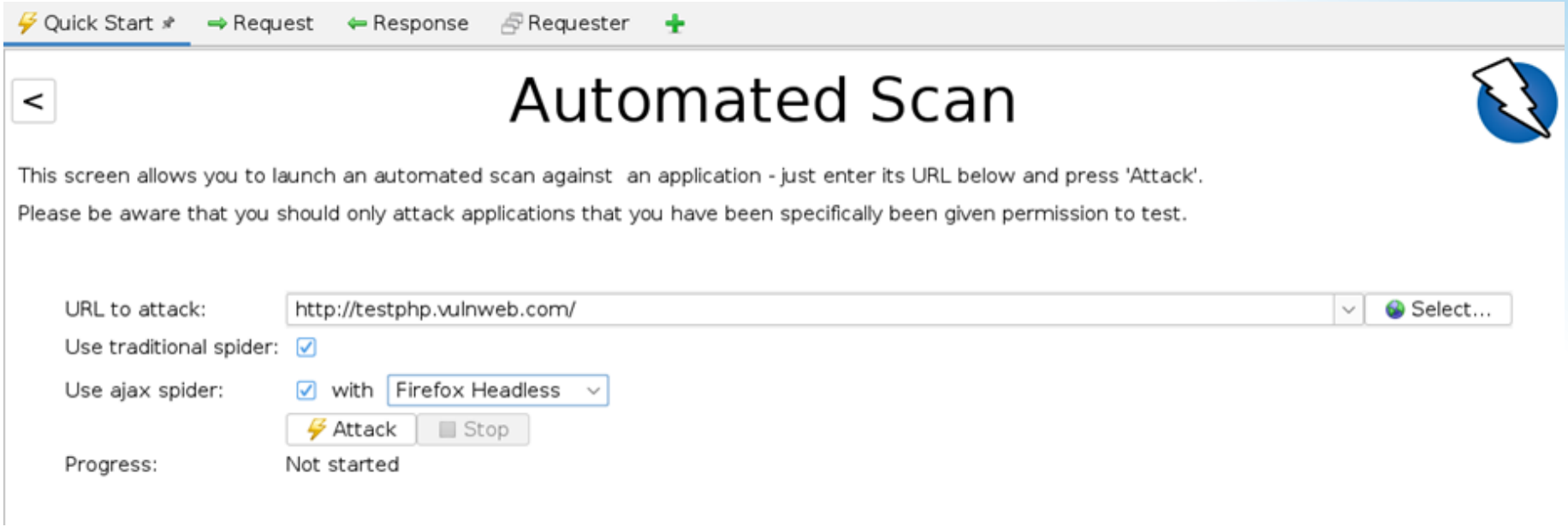


"Zed Attack Proxy"

Stable release	2.14.0[1] / 12 October 2023; 8 months ago
Repository	github.com/zaproxy/zaproxy
Written in	Java
Operating system	Linux, Windows, OS X
Available in	25[2] languages
Type	Computer security
License	Apache Licence
Website	www.zaproxy.org

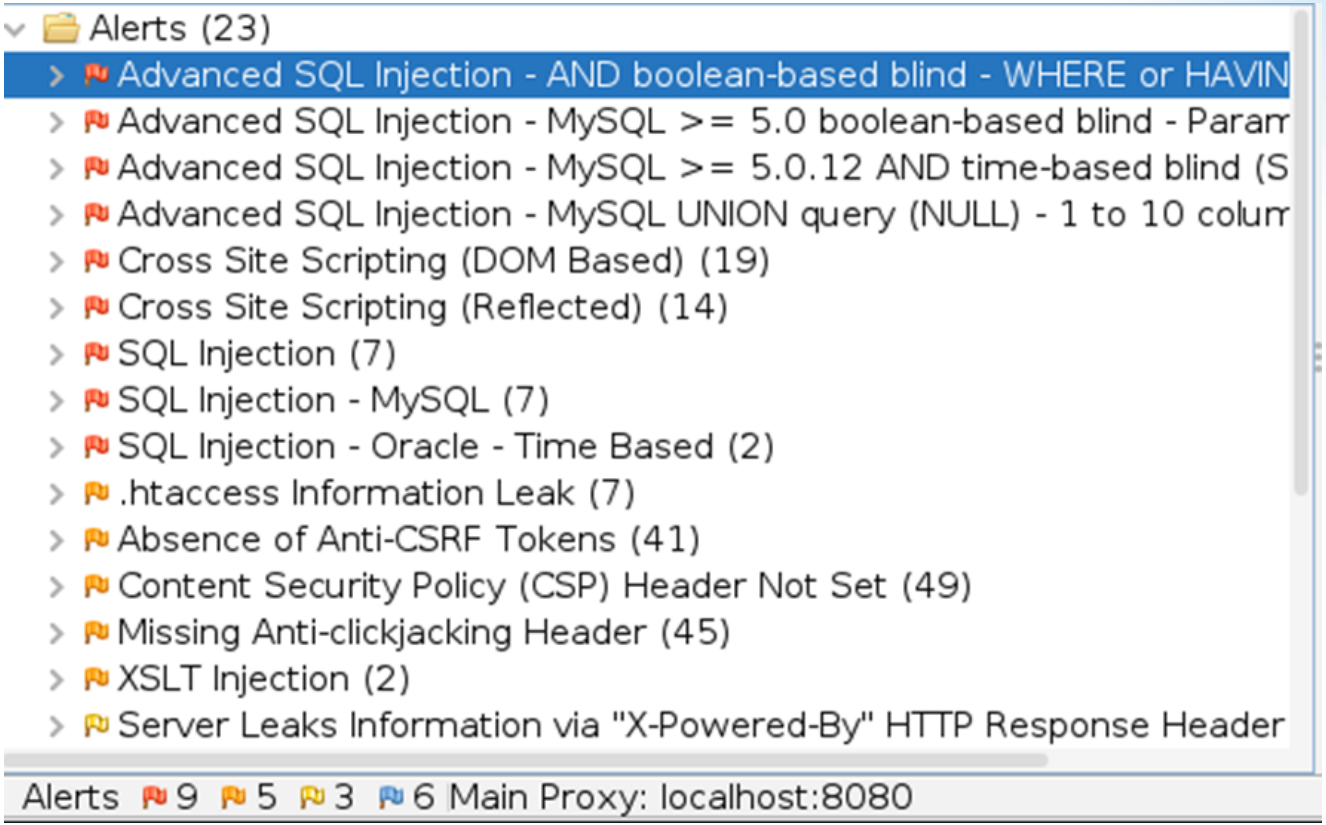
EPIC
Institute of Technology
Powered by epam

Attack



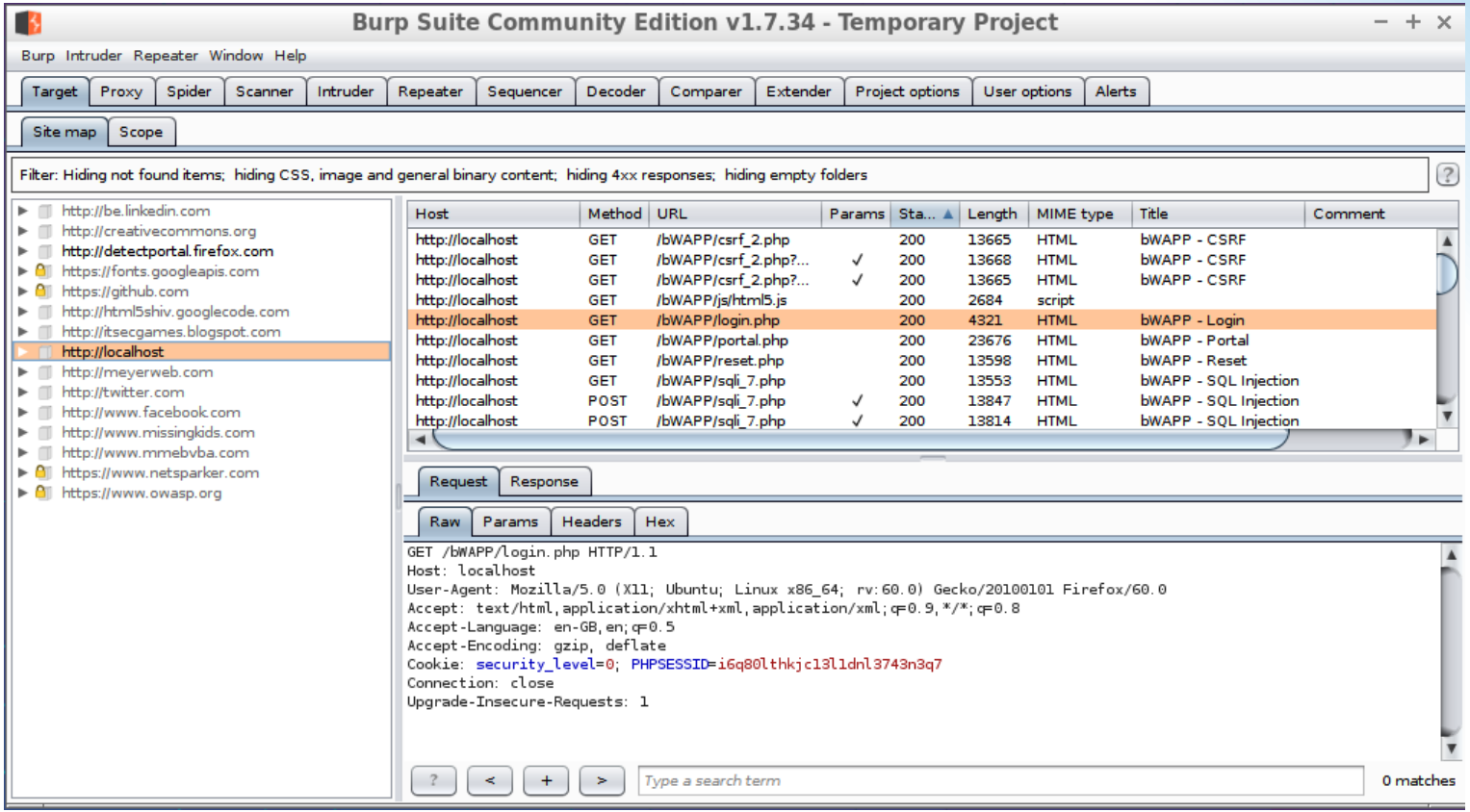
EPIC
Institute of Technology
Powered by epam

Alerts



EPIC
Institute of Technology
Powered by <epam>

Burp Suite



EPIC
Institute of Technology
Powered by epam

ZTA

the face of a network viewed as compromised. A zero trust architecture (ZTA) is an enterprise's cyber security plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.

There are several ways to implement all the tenets of ZT; a full ZTA solution will include elements of all three:

- Using enhanced identity governance and policy-based access controls.
- Using micro-segmentation
- Using overlay networks or software-defined perimeters

EPIC
Institute of Technology
Powered by epam

Bug bounty

Bug bounty program

16 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

A **bug bounty program** is a deal offered by many websites, organizations, and software developers by which individuals can receive recognition and compensation[1][2] for reporting bugs, especially those pertaining to security exploits and vulnerabilities.[3]

These programs allow the developers to discover and resolve bugs before the general public is aware of them, preventing incidents of widespread abuse and data breaches. Bug bounty programs have been implemented by a large number of organizations, including Mozilla,[4][5] Facebook,[6] Yahoo!,[7] Google,[8] Reddit,[9] Square,[10] Microsoft,[11][12] and the Internet bug bounty.[13]

Companies outside the technology industry, including traditionally conservative organizations like the United States Department of Defense, have started using bug bounty programs.[14] The Pentagon's use of bug bounty programs is part of a posture shift that has seen several US Government Agencies reverse course from threatening white hat hackers with legal recourse to inviting them to participate as part of a comprehensive vulnerability disclosure framework or policy.[15]

Appearance hide

Text

- Small
- Standard
- Large

Width

- Standard
- Wide

EPIC
Institute of Technology
Powered by epam

That's All Folks!